AO 91 (Rev. 11/11) Criminal Complaint

Sealed
Public and unofficial staff access to this instrument are prohibited by court order

UNITED STATES DISTRICT COURT

for the

District of Puerto Rico

4:21-mj-2219

United States of America
v.
Oluwasegun Baiyewu

Case No. 21-1261 (MJ)

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of October 27, 2020 in the county of Carolina in the _____ District of Puerto Rico, the defendant violated:

Code Section	*Offense Description*
18 USC 1343	Wire Fraud
18 USC 1349	Conspiracy to Commit Wire Fraud
18 USC 1956(a)(1)(B)(i)	Money Laundering

This criminal complaint is based on these facts:

See Attached Affidavit.
Approved by SAUSA John Auchter.

John Auchter

☑ Continued on the attached sheet.

Complainant's signature

Special Agent Marc Smith
Printed name and title

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at: 3:46pm

Date: 10/13/2021

Judge's signature

City and state: San Juan, Puerto Rico

U.S. Magistrate Judge Marshal D. Morgan
Printed name and title

AFFIDAVIT IN SUPPORT OF COMPLAINT AND ARREST WARRANT

I, Marc Smith, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since 2017. I am assigned to the FBI San Juan Division Cyber Crimes Investigation Task Force. I have received training and investigated a variety of federal crimes involving cyber intrusion and computer fraud. I have experience regarding these federal violations through my daily investigative responsibilities and extensive training. For example, I have attended numerous classes and trainings dealing with computer crimes and fraud, including how computer networks operate, methods employed by criminals to infiltrate computer networks and commit other crimes, the purpose of the intrusions, and the numerous types of fraudulent schemes that perpetrators of computer crimes carry out after gaining access to computer networks (e.g., selling stolen credit card information located on a compromised computer or surreptitious use of a compromised computer for further intrusions).

2. I have conducted numerous complex investigations concerning computer crimes and fraud, including wire and mail frauds, intrusions (i.e., gaining access to a protected computer or computer network without permission), denial of service attacks (i.e., attempts to make a website, computer, or device unresponsive), the use of botnets (i.e., a group of computers controlled without the knowledge of the computers' owners), and the use of bulletproof servers (i.e., servers controlled by administrators who often are non-responsive to law enforcement requests and often host illicit content anonymously). I have extensive experience reviewing records related to computer crime and fraud, including Internet Protocol ("IP") address logs used

by computers on the Internet, network access logs, and security programs. I also have extensive experience debriefing defendants, witnesses, informants, and other persons involved in computer crime and fraud. I have personally conducted and have been involved in numerous investigations that included the execution of search warrants involving electronic evidence and have been involved in all phases of investigations, from inception through trial, of computer intrusions as well as of criminal hackers. I have earned credentials from the Association of Certified Fraud Examiners, the Information Systems Audit and Control Association, the International Information System Security Certification Consortium, and the Global Information Assurance Certification.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe Oluwasegun Baiyewu ("**Baiyewu**") has committed violations of 18 U.S.C. §§ 1343, 1349, and 1956(a)(1)(B)(i). Therefore, I respectfully request the Court approve the requested complaint and arrest warrant.

FACTS ESTABLISHING PROBABLE CAUSE

The BEC Conspiracy

5. Since about March 2018, a criminal conspiracy has targeted victim businesses with business email compromise ("BEC") schemes. A BEC is a type of online scam targeting

victim businesses which conduct banking transactions and wire transfers online. In a BEC, an individual obtains unauthorized access to the email accounts of one or more business entities and then observes email traffic to identify financial transactions; inserts him or herself into that transaction by using a spoofed[1] email address or domain; and, using the spoofed email address, manipulates an employee of the victim business to change the payee bank account information for an account slated to receive payment from a victim business. The payment is sent to a bank account controlled by a member of the BEC conspiracy, rather than the bank account held by the actual, legitimate payee.

6. The conspiracy recruits money mules to launder the funds fraudulently obtained by having the money mules create fictitious businesses and open a variety of business bank accounts at U.S. financial institutions. The fictitious businesses do not engage in any legitimate business activity and are created by the conspiracy solely to launder funds. Funds are laundered to and distributed amongst certain members of the BEC conspiracy located overseas via monetary transactions or via the purchase of vehicles which are then exported to another country—often, Nigeria—and sold in that destination country.

7. On August 13, 2020, a grand jury in the Southern District of New York returned a superseding indictment against certain persons involved in the BEC conspiracy for violations of 18 U.S.C. §§ 1349 and 1956(h). *See U.S. v. Uko, et. al*, No. 1:20-cr-179-DLC, ECF No. 113 (S.D.N.Y. Aug. 13, 2020). As alleged in the indictment and superseding indictment in *U.S. v.*

---

[1] Spoofing is a technique where an email address is created so it appears to be from a legitimate sender. In other words, if a conspirator wished to make it appear an email came from a legitimate government source, the domain would be listed as "@fbi.gov.com" or "@fbi.com" instead of "@fbi.gov."

Uko, et. al, between March 2018 and January 2020, members of the BEC conspiracy conspired to launder proceeds which had been fraudulently obtained from a variety of BEC schemes. *See id.* at ECF Nos. 18, 113. Of the 14 defendants charged in *U.S. v. Uko, et. al*, nine have pled guilty to 18 U.S.C. § 1956(h) and have been sentenced or are pending sentencing. *See id.* at ECF Nos. 257, 290, 338, 343, 351, 375, 376, 407, 423, 427. One other defendant was found guilty following a jury trial. *See id.* at ECF No. 299. Two of the defendants, Collins Eneh ("Eneh") and Ndukwe Anyaogu, fled the jurisdiction of the U.S. and remain fugitives.

8. Current members of the BEC conspiracy consist of **Baiyewu**, Eneh, Blossom Eghaghe ("Eghaghe"), Michael Crosby ("Crosby"), and others.

9. **Baiyewu** is a Nigerian national and long-term permanent resident who resides in Richmond, Texas. **Baiyewu** incorporated the legal entity Shipopo LLC ("Shipopo") in Texas on or about April 29, 2020. **Baiyewu**'s residence is listed as Shipopo's principal place of business. **Baiyewu** uses Shipopo to launder funds to certain conspirators located overseas by exporting vehicles purchased from Copart, Inc. ("Copart") to Nigeria. From May 2020 through December 2020, **Baiyewu** used Shipopo to export 17 vehicles to Eghaghe in Nigeria. On six separate occasions in 2020, **Baiyewu** delivered 31 money orders totaling $30,088 to Copart to apply to account #877801 for vehicle auctions which Eghaghe had won. It is believed the cashier's checks which **Baiyewu** delivered consisted solely of the proceeds of BEC schemes involving different victims. Based on my training and experience, I know that money orders are frequently purchased by money mules in amounts of between $500 and $1,000. Money mules obtain or are instructed to obtain instruments in these amounts to evade reporting requirements and prevent law enforcement detection of money laundering activity. Money orders are attractive to money launderers because identification documents are not required to purchase them, thus they provide

an anonymous way to tender value. The money orders are typically provided by their purchasers to others who conduct additional transactions with money orders to attenuate the link between fraud proceeds and the recipient or recipients of the proceeds. In addition, I know and have observed in this investigation that members of the conspiracy under investigation often "convert" funds obtained by fraud through a series of transactions into cash to obscure the source of the funds, and then further obscure the relationship between the cash and the fraud by re-depositing it into different bank accounts.

10. Eneh is a money broker who works on behalf of certain members of the BEC conspiracy to launder proceeds. Eneh is notified by certain conspirators who have obtained unauthorized access to the email accounts of victim businesses about funds which are about to be fraudulently diverted. Eneh then contacts money mule recruiters to see which accounts are available to launder the funds and directs the laundering of the funds depending on the responses Eneh has received from the money mule recruiters.

11. Eghaghe is a Nigerian national. Eghaghe maintains accounts with several online vehicle auction and remarketing companies, including Copart. Eghaghe owns and controls Copart account #877801. Eghaghe uses Copart account #877801 to purchase vehicles located throughout the U.S. using funds fraudulently obtained by the BEC conspiracy. Eghaghe then directs other conspirators, including **Baiyewu**, to export these vehicles to Nigeria. Once the vehicles are imported into Nigeria, Eghaghe and certain other members of the BEC conspiracy sell the vehicles and distribute the proceeds amongst members of the conspiracy.

12. Crosby was introduced to Eneh in about late 2019 by Joshua Fitten ("Fitten"), a member of the BEC conspiracy who was charged, pled guilty, and has been sentenced in the Southern District of New York matter. *See id.* at ECF Nos. 18, 407. Crosby recruits money

mules located in the California area to open bank accounts to launder the funds fraudulently obtained by the BEC conspiracy. Crosby also helps launder funds to certain conspirators located overseas via monetary transactions or via the purchase of vehicles from Copart, which are then exported to Nigeria and sold or used by conspirators.

The Puerto Rico BEC Scheme

13. In about October 2020, a company based in Carolina, Puerto Rico ("**Victim G.I.**") was targeted by the BEC conspiracy. A conspirator compromised the email accounts for **Victim G.I.** and started to monitor email traffic between **Victim G.I.**'s employees and **Victim G.I.**'s vendors.

14. On or about October 21, 2020, Crosby directed a money mule ("Account Holder A") to open a fictitious business. Crosby also directed Account Holder A to open a business account in the name of the fictitious business at JPMorgan Chase Bank, N.A. ("Account xxxxxx1959") for the purpose of laundering illicit funds derived from BEC schemes.

15. On or about October 23, 2020, Eneh sent a message to Crosby: "[e]xpecting [$]159k and [$]150k" and asked whether Crosby had an account ready to accept these ACH deposits. Crosby told Eneh that Account xxxxxx1959 was available to accept ACH deposits. On or about October 26, 2020, Eneh again confirmed to Crosby**:** "[w]e expecting 3 drops this week" to Account xxxxxx1959.

16. On or about October 27, 2020, a conspirator sent a spoofed email to one of **Victim G.I.**'s employees. This email directed the employee to wire $112,129.53 to Account xxxxxx1959. The funds were intended to be paid to **Victim G.I.**'s vendor, but Account xxxxxx1959 was not in any way associated with the vendor and was solely used by members of

the conspiracy to launder funds stolen via BEC schemes. **Victim G.I.**'s employee did wire the funds from **Victim G.I.**'s bank account located in Puerto Rico to Account xxxxxx1959.

17. On or about October 27, 2020, Crosby sent a screenshot to Eneh showing the BEC conspiracy had succeeded in fraudulently diverting the funds from **Victim G.I.**

18. On or about November 5, 2020, a conspirator sent another spoofed email to one of **Victim G.I.**'s employees. This email directed the employee to wire approximately $102,000, but this transfer was frozen and returned by the recipient bank due to the recipient bank's concern the funds had been fraudulently diverted.

The Laundering of the Puerto Rico BEC Scheme Proceeds

19. On or about October 27, 2020, Eneh directed Crosby to purchase four cashier's checks to launder the funds fraudulently obtained from **Victim G.I.** Of these four cashier's checks, Eneh directed Crosby to make out one to Copart in the amount of $31,126. Eneh explained this cashier's check should be applied to Copart account #877801, lot #47680680 and 44632770. Lot #47680680 was a 2014 Land Rover Range Rover located in Atlanta, Georgia, and Lot #44632770 was a 2006 Toyota Sienna located in Minneapolis, Minnesota.

20. On or about October 28, 2020, when Crosby and Account Holder A were purchasing cashier's checks, employees of JPMorgan asked about the source of the funds in Account xxxxxx1959. Crosby messaged to Eneh: "bro they are not letting [Account Holder A] get anymore cash out the[y're] saying they need to verify w[h]ere it came from answer." Eneh confirmed: "Puerto Rico. That's w[h]ere the money came from." Crosby and Account Holder A were able to successfully purchase all four cashier's checks after providing information on the source of funds.

21. On or about October 29, 2020, Crosby delivered the cashier's check made out to Copart to a Copart location in Wilmington, California. Crosby sent Eneh a photo of the sales receipt which Crosby received from Copart, showing the balance for the 2014 Land Rover Range Rover and 2006 Toyota Sienna had been satisfied.

22. Between on or about October 29 and October 30, 2020, Crosby cashed the three other cashier's checks which had been made payable to individuals. Crosby then provided this bulk U.S. currency, less Crosby's fee, to members of the BEC conspiracy so it could be further laundered and distributed amongst the conspirators.

23. On or about October 20, 2020, and prior to Crosby paying the remaining balance on the 2014 Land Rover Range Rover, Eghaghe had sent a 4 million Nigerian Naira (approximately $9,700) wire transfer to **Baiyewu** with the memo "[f]urther deposit toward payment for $30k Range Rover." These funds represent the proceeds of a BEC scheme involving a different victim. On or about October 22, 2020, **Baiyewu** made a payment to Copart of $2,996 which consisted of two $1,000 MoneyGram money orders and one $996 Kroger money order. A portion of this payment was applied to the 2014 Land Rover Range Rover.

24. On or about November 2, 2020, **Baiyewu** and other members of the BEC conspiracy picked up the 2014 Land Rover Range Rover and 2006 Toyota Sienna from their respective locations and prepared them for exportation.

25. On or about November 10, 2020, **Baiyewu** and other members of the BEC conspiracy exported the 2006 Toyota Sienna to Nigeria.

26. On or about November 14, 2020, **Baiyewu**, Eghaghe, and other members of the BEC conspiracy exported the 2014 Land Rover Range Rover to Nigeria.

27. On or about November 25, 2020, **Baiyewu** visited a Navy Federal Credit Union branch in Sugarland, Texas and attempted to deposit $12,735 in U.S. currency into **Baiyewu**'s account no. xxxxxx4548. When the teller informed **Baiyewu** that Navy Federal Credit Union would report this deposit to the government in a Currency Transaction Report as it was more than $10,000, **Baiyewu** refused to complete the deposit and insisted on the return of the currency. A representative of Navy Federal Credit Union confirmed that **Baiyewu** is known to deposit large amounts of U.S. currency, typically just below the reporting threshold of $10,000. Based on my training and experience, **Baiyewu**'s deposit activity is indicative of structuring intended to avoid reporting requirements and law enforcement detection of money laundering activity.

CONCLUSION

28. Based on the forgoing, there is probable cause to believe **Baiyewu** committed violations of 18 U.S.C. §§ 1343, 1349, and 1956(a)(1)(B)(i) by conspiring with Eneh, Eghaghe, Crosby, and others to fraudulently divert a wire transfer of 112,129.53 from **Victim G.I.** and then launder a portion of those funds through the purchase of two vehicles which were exported to Nigeria.

REQUEST FOR SEALING

29. I further request that the Court order that all papers in support of this application, including the affidavit and arrest warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation. As discussed above, certain targets of the investigation fled the jurisdiction of the U.S. and are fugitives in related matters. Accordingly, there is good cause to

seal these documents because their premature disclosure may give targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify co-conspirators, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Marc Smith
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me pursuant to FRCP 4.1 at 3:46PM by telephone, this 13th day of October 2021.

United States Magistrate Judge Marshal D. Morgan
District of Puerto Rico